GRUPO MERCANTIL

Política de Segurança Cibernética

Vigência a partir de: 09/04/2026
Validade: 1 ano
Versão: 04

Divulgação Externa

Sumário

1. APRESENTAÇÃO 3
2. DIRETRIZES 3
2.1. Critérios e acionamentos 3
2.2. Direito de propriedade 5
2.3. Definição de relevância e conceitos gerais 5
2.4. Relatório e Reporte 6
2.5. Comunicação dos incidentes relevantes 6
2.6. Compartilhamento de informações sobre os incidentes relevantes 7
2.7. Auditoria e Monitoramento 8
2.8. Prevenção e tratamento do vazamento de informações 8
2.9. Cultura e treinamento em Segurança Cibernética e da Informação 9
2.10. Gestão de fornecedores/empresas prestadoras de serviços de TI 10
2.11. Gestão de vulnerabilidades 10
2.12. Segurança Antimalware 11
2.13. Classificação da Informação 11
2.14. Gestão da Criptografia 11
2.15. Contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior 12
2.15.1. Serviços de Comunicação (RSFN) 13
2.16. Interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior 13
2.17. Monitoramento de Conexões com Ambientes Externos e Eventos Atípicos 13
2.17.1. Critérios de Alerta 14
2.17.2. Caracterização de Eventos Atípicos 14
2.17.3. Tratamento e Resposta 14
2.17.4. Registros e Evidências 14
2.18. Disponibilidade e Retenção de Mecanismos de Controle (Compliance BACEN) 14
2.18.1. Abrangência da Documentação 15
2.18.2. Prazo de Guarda e Contagem: 15
2.18.3. Condições de Armazenamento 15
2.19. Segurança nas Conexões com Sistemas do Mercado Financeiro 15
2.20. Uso de Correio Eletrônico e Dispositivos Móveis 16
2.21. Descarte Seguro de Informações 16
2.22. Acesso a Dados e Sistemas 17
2.23. Acesso e Uso de Recursos da Internet 17
2.24. Credenciais Privilegiadas de Administrativas 18
2.25. Senhas de Acesso à Rede Corporativa 18
2.26. Pentest e Teste de Vulnerabilidade 19
2.26.1. Plano Simulado de Ataques Ciberneticos 19
2.27. Gestão de Vulnerabilidades e Patch Management 19
2.28. Acesso Remoto a Rede Corporativa do Grupo Mercantil 20
2.29. Plano de Ações de Respostas a Incidentes 21

Divulgação Externa

2.29.1. Checklist de Acoes de Seguranca Cibernetica 22
3. PAPÉIS E RESPONSABILIDADES 22
4. CONSIDERAÇÕES FINAIS 24
5. REFERÊNCIAS NORMATIVAS 24
6. GLOSSÁRIO 24

Divulgação Externa

1. APRESENTAÇÃO

A presente Política é aplicável a todos que estão indicados no item "Abrangência" deste documento.

No contexto atual em que cada dia mais as organizações estão suscetíveis a ataques provenientes do espaço cibernético, é necessário que sejam adotadas medidas com o objetivo de detectar, identificar, proteger e responder rapidamente a tais situações.

Esta Política tem como premissa a proteção das informações da organização, seus clientes e partes interessadas de forma a preservar os seguintes princípios, sem prejuízo da garantia de Autenticidade, Irretratabilidade (Não repúdio) e Legalidade:

- Confidencialidade: Garantia de que a informação não será acessada ou revelada a indivíduos, entidades ou processos não autorizados.

- Integridade: Garantia de que a informação não sofreu alteração indevida, assegurando a salvaguarda da exatidão e completeza da informação.

- Disponibilidade: Garantia de que a informação estará acessível aos colaboradores autorizados sempre que necessário.

A Política Institucional de Segurança Cibernética deve ser divulgada aos funcionários da instituição e às empresas prestadoras de serviços, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações. Ressalta-se ainda que as diretrizes e a estrutura contemplada nesse documento foram desenhadas em compatibilidade com a natureza, o porte, a complexidade dos produtos, serviços, processos e atividades, bem como ao perfil de risco e o modelo de negócio da Instituição.

Um resumo deve ser divulgado ao público contendo as linhas gerais da política de Segurança Cibernética.

2. DIRETRIZES

2.1. Critérios e acionamentos

Os procedimentos para tratamento de incidentes visam identificar os eventos ocorridos no ambiente e as ações corretivas para o seu tratamento, buscando garantir a não recorrência de eventos. As atividades de tratamento de incidentes de segurança da informação e cibernética estão distribuídas matricialmente. O procedimento é centralizado na figura do Coordenador de Segurança da Informação, responsável por coordenar as atividades dos diversos grupos e especialistas.

Se mais de um ataque cibernético estiver ocorrendo ao mesmo tempo, os ataques devem ser priorizados, já que a organização provavelmente não terá o tempo e os recursos para enfrentar todas as ameaças ao mesmo tempo.

Divulgação Externa

Os incidentes devem ser categorizados e priorizados com base no impacto potencial (conforme procedimento operacional interno - política de avaliação de risco de segurança da informação) que pode ter sobre a organização e no tempo e recursos necessários para se recuperar.

O impacto pode incluir o impacto do ataque na funcionalidade do negócio, bem como o impacto que ele tem sobre a informação da organização.

Impactos nos processos de negócio:

Impacto	Descrição
BAIXO	• Funções comerciais críticas e não críticas funcionam normalmente • Incidentes causam nenhuma ou pouca interrupção na função ou na prestação de serviços crítica do negócio Muito pouco ou nenhuma interrupção na prestação de serviços Esse nível representa operações típicas do dia a dia. Podem ocorrer tentativas de incidentes em um sistema de informação não crítico; no entanto, os controles, como um scanner de vírus, impedem que isso ocorra e removam a ameaça. Se um sistema não crítico for infectado, o serviço de proteção da organização pode remover a ameaça e restaurar o sistema para as operações normais. Não é necessária nenhuma escalação para a Equipe de Resposta a Incidentes.
MÉDIO	• Impacto em um pequeno número das funções críticas do negócio da organização • Incidentes causam uma pequena interrupção na entrega do serviço, dependendo do (s) sistema (s) impactado (s) Interrupção menor na prestação de serviços Este nível representa um estado de alerta. Alguns sistemas de informação críticos e não críticos podem ser impactados por um incidente. Escalação para a equipe de resposta ao incidente será necessária para ajudar a avaliar a situação e mitigar o impacto da exposição. Se a Equipe de Resposta a Incidentes e as partes interessadas relevantes decidirem que não houve impacto nas funções críticas do negócio da organização, elas podem responder implementando atividades de emergência ou solicitando um processo de gerenciamento de patches de emergência.

Divulgação Externa

ALTO	• A maioria das funções críticas do negócio da organização são impactadas • Incidentes causam uma grande interrupção na entrega do serviço, violação de dados ou destruição de dados para os sistemas de informação; Grande Perturbação na Entrega de Serviços / Incidentes de Segurança Cibernética Catastrófica Esse nível indica que a atenção imediata da Equipe de Resposta a Incidentes é necessária. Os sistemas críticos de informação podem ser comprometidos ou destruídos juntamente com dados críticos. Este nível desencadeará uma resposta centralizada e coordenada por partes interessadas na organização. As partes interessadas externas, tais como fornecedores que se especializam em resposta a incidentes, podem estar envolvidas.

Para maiores informações, poderá ser consultado o procedimento de "Plano de Ações de Respostas a Incidentes de Segurança Cibernética de TI", que está vinculado a Política Institucional de Segurança Cibernética.

2.2. Direito de propriedade

Toda informação gerada ou processada pelas empresas do Grupo Mercantil e que possua consenso das partes envolvidas será considerada propriedade e ativo importante para o negócio, sendo de sua responsabilidade implementar controles que garantam níveis adequados de proteção.

2.3. Definição de relevância e conceitos gerais

- Entende-se como informações relevantes qualquer informação que contenha dados pessoais (informação relacionada a pessoa física ou jurídica identificada ou identificável) e/ou dados pessoais sensíveis (dado genético ou biométrico) de clientes de quaisquer empresas financeiras do grupo Mercantil.

- Define-se como serviços relevantes os serviços prestados por terceiros que armazenam ou processam dados relevantes.

- Classifica-se como incidente relevante todos os incidentes que envolvem informações e/ou serviços relevantes.

- Classifica-se como crise ataques e ações internas ou externas visando cenários que forcem ou resultem em vazamento de dados, negação de serviço, técnicas de malware, acessos não autorizados, engenharia social.

- Classificam-se como incidente um evento ou conjunto de eventos confirmados ou sob suspeita visando impactar a disponibilidade, integridade e confidencialidade dos ativos e informações da instituição.

Divulgação Externa

2.4. Relatório e Reporte

O relatório deve ser realizado como forma de documentar e armazenar informações que servirão como referências para futuros casos, forma de aprender sobre o ocorrido, bem como ser usadas como evidência para quaisquer questões legais que poderão ocorrer.

Deverá constar no relatório:

- O tipo e a natureza do incidente;
- Se o incidente poderia ou não ter sido impedido;
- Como e quando o incidente foi detectado e se alguma melhoria nas ferramentas de detecção é necessária;
- Os sistemas afetados pelo ataque;
- Como a organização respondeu ao ataque e o que poderia ter sido feito melhor durante o processo de resposta ao incidente.

O reporte deverá ocorrer conforme o fluxo definido na Política de Segurança da Informação, na qual deverão ser seguidos a quem, como e quando comunicar. Em casos de incidentes deverão ser reportados aos:

- Órgãos reguladores os incidentes cibernéticos, conforme os critérios adotados para escalonamento e classificação de criticidade;
- Ao Banco Central e ao mercado a ocorrência de incidentes relevantes;
- Canais específicos para a finalidade de incidentes de Segurança Cibernética e informação.

2.5. Comunicação dos incidentes relevantes

Conforme determinado pela Resolução CMN Nº 4.893/21, as empresas financeiras do grupo Mercantil devem comunicar ao Banco Central do Brasil a ocorrência de incidentes cibernéticos classificados como relevantes, bem como demais incidentes que o Comitê de TI possa entender como significativos de forma a afetar suas atividades em todo território nacional.

A deliberação e categorização dos incidentes deverão ser realizada pelo Comitê de TI através de atas, ocorrendo de forma extraordinária ou através das reuniões regulares.

A comunicação dos incidentes classificados como relevantes deve ser realizada através do SISCOM WEB disponibilizado pelo Banco Central do Brasil e será feita exclusivamente pelo Diretor responsável pela Segurança Cibernética, contemplando todas as informações existentes sobre o referido incidente.

Divulgação Externa

2.6. Compartilhamento de informações sobre os incidentes relevantes

As iniciativas para compartilhamento de informações sobre os incidentes relevantes, são mencionadas no inciso III do art. 20 da Resolução CMN Nº 4.893/21, BCB Nº 85/21 e Resolução CVM Nº 35/21, em que as empresas financeiras do grupo Mercantil autorizadas a funcionar devem:

- Adotar os procedimentos para gerenciamento de riscos previstos na regulamentação em vigor devem especificar, no tocante à continuidade dos serviços de pagamento prestados:

  - O tratamento previsto para mitigar os efeitos dos incidentes relevantes, tais como o registro, a análise da causa e do impacto;

  - O prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos;

  - Comunicar tempestivamente ao Banco Central do Brasil e as demais empresas do sistema financeiro nacional as ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, que configurem uma situação de crise pela instituição financeira, bem como das providências para o reinício das suas atividades.

  - Comunicar à SMI e aos órgãos de administração, BSM e B3 a ocorrência de incidentes relevantes que afetem seus sistemas críticos e tenham impacto significativo sobre os clientes. A comunicação de que trata a Resolução CVM Nº 35/21, deve conter:

    - A descrição do incidente, indicando de que forma os clientes foram afetados;

    - Avaliação sobre o número de clientes potencialmente afetados;

    - Medidas já adotadas pelo intermediário ou as que pretende adotar;

    - Tempo consumido na solução do evento ou prazo esperado para que isso ocorra; e

    - Qualquer outra informação considerada importante.

  - Deve ainda manter à disposição da SMI cópia:

    - Das comunicações realizadas com seus clientes, se houver; e

    - Dos relatórios internos de investigação produzidos pelo intermediário ou por terceiros sobre a análise do incidente e as conclusões dos exames efetuados.

O processo de registro, análise da causa, impacto, prazos para reinício e controles de incidentes relevantes é regida por procedimento específico que define as ações próprias. Esse procedimento como título – "Plano de Resposta a Incidente de Segurança Cibernética", pode ser consultada na Política de Segurança da Informação.

Divulgação Externa

As informações antes de serem oficialmente compartilhadas, devem ser submetidas ao Diretor responsável pela Segurança Cibernética, bem como ao Comitê de Riscos para avaliação e comunicação aos órgãos competentes.

As informações também deverão estar disponibilizadas ao Conselho de Administração do Banco Mercantil, e caberá ao Diretor de Segurança Cibernética e ao Comitê de Riscos, o agendamento/convocação para a devida apresentação.

2.7. Auditoria e Monitoramento

Para garantir a utilização adequada dos serviços oferecidos por terceiros às empresas do grupo Mercantil, o Diretor responsável pela Segurança Cibernética e as demais áreas envolvidas se reservam-se ao direito de realizar auditorias internas e externas, bem como o monitoramento em todos os ativos e serviços de tecnologia da informação, em qualquer tempo, sem a necessidade de aviso prévio ao prestador.

Os mecanismos de acompanhamento e de controle serão realizados de forma automatizada sempre que possível, através de softwares especialistas com vistas a assegurar a implementação e a efetividade da Política de Segurança Cibernética, do Plano de Ação e de resposta a incidentes. O processo de monitoramento contínuo do ambiente irá garantir a manutenção dos controles para a identificação de vulnerabilidades quando da ocorrência de incidentes.

Os fornecedores/empresas prestadoras de serviços a terceiros relevantes deverão comprovar os mecanismos utilizados para o monitoramento do seu ambiente de TI. Na ocorrência de um incidente com os dados do Banco Mercantil, o mesmo deve ser comunicado imediatamente à área gestora para acompanhamento e demais providências conforme descrito no Plano de Resposta a Incidente de Segurança Cibernética, constante da Política de Segurança da Informação.

2.8. Prevenção e tratamento do vazamento de informações

É de suma importância que os funcionários, parceiros e terceiros a quem essa política se aplica, se conscientizem sobre o processo de classificação da informação, bem como sejam capacitados através do treinamento em Segurança Cibernética e da Informação.

O Banco Mercantil adota várias formas de prevenção ao vazamento de dados pessoais, utilizando técnicas e ferramentas voltadas para:

- Classificação de documentos, mensagens e e-mails.
- Controle de envio e/ou compartilhamento de informações internas, baseadas em políticas e regras de prevenção a perda de dados.
- Bloqueio de portas USB para dispositivos Mass Storage (pen-drive, HD externo).
- Bloqueio de acesso a site de armazenamento de informações em nuvem (cloud), tais como drivers (Google, Microsoft, DropBox).
- Bloqueio de envio de arquivos classificados como anexo em serviços de e-mail público, tais como Gmail, Outlook, Yahoo, etc.
- Bloqueio de informações dispostas em imagem de sistemas interno do Grupo Mercantil, seja em cópias locais de pen-drive, ou envios por meio serviço na internet.

Divulgação Externa

- Uso do serviço de e-mail seguro do Grupo Mercantil (Secmail), para destinatários previamente selecionados que tratam de informações privilegiadas ou sensíveis.

- Uso de transporte de dados seguros por meio de protocolos como HTTPS, SFTP, FTPS

Os arquivos internos, ao serem transportados ou transmitidos por meio de mídias removíveis, devem ser submetidos a processos de criptografia para assegurar a confidencialidade e integridade das informações. A utilização de algoritmos de criptografia aprovados e a implementação de chaves seguras são práticas essenciais para proteger os dados contidos nessas mídias durante seu deslocamento, minimizando os riscos de acesso não autorizado e interceptação indevida.

A Agência Nacional de Privacidade de Dados – ANPD, é o órgão da administração pública empenhada no compromisso de construir um ambiente de respeito aos direitos dos titulares dos dados e, ainda, de zelar pela proteção dos dados pessoais de cada cidadão brasileiro.

Como forma de padronizar o fluxo de tratamento, processamento e casos de incidentes envolvendo dados pessoais, a ANPD indica vários pontos importantes, como:

- Formas de avaliar o incidente de dados pessoais.

- Formas de comunicar a ANPD e aos titulares dos dados envolvidos.

- Elaborar documentação e relatórios voltados para análise de possíveis incidentes de dados.

É citado no procedimento de Plano de Ações de Respostas a Incidentes de Segurança Cibernética de TI, as formas de comunicação interna, fluxos de tomadas de decisão, bem como planos de respostas envolvendo incidentes de dados pessoais.

2.9. Cultura e treinamento em Segurança Cibernética e da Informação

Um dos pontos mais importantes para a proteção da informação é a disseminação da cultura de Segurança Cibernética e da Informação e, por esse motivo, o Banco Mercantil implementa um programa de capacitação e avaliação, divulgando as políticas de segurança da informação a todos os seus colaboradores e também para o público em geral.

As abordagens deverão ser realizadas através de campanhas onde estão autorizados os formatos de phishing, smishing, vishing, webinar, vídeos de conscientização, apresentações, elaboração de materiais gráficos e dicas rápidas.

Para garantir a efetividade das campanhas, as mesmas devem desenvolver mecanismos capazes de mensurar: áreas mais vulneráveis; detalhamento das áreas e usuários que foram vítimas por campanha; top usuários reincidentes; detalhamento dos usuários que não concluíram com sucesso o treinamento; detalhamento dos usuários que não tiveram uma nota satisfatória no quiz; engajamento dos usuários em cada campanha de treinamento; informações detalhadas de cada campanha.

Divulgação Externa

Os clientes devem ser informados sobre os riscos relacionados às práticas de segurança cibernética aplicadas ao sistema financeiro. Os mesmos devem estar cientes:

- Das atividades aderentes aos requerimentos e padrões adotados pelas empresas do grupo Mercantil, relacionados a confidencialidade, integridade e disponibilidade dos seus dados;

- Sobre precauções na utilização de produtos e serviços financeiros;

- Sobre a coleta, tratamento e manutenção de suas informações em bases de dados.

2.10. Gestão de fornecedores/empresas prestadoras de serviços de TI

Todos os fornecedores/empresas prestadoras de serviços de TI, que processam e/ou armazenam dados relevantes das empresas financeiras do grupo Mercantil em data center próprio ou na modalidade de nuvem, serão submetidos à avaliação de controles de segurança da informação e segurança cibernética para que seja possível identificar sua maturidade quanto às diretrizes desta política e também definir suas responsabilidades e papéis dentro dos processos para o qual o serviço será prestado.

Processos de avaliação e monitoramento de fornecedores/empresas prestadoras de serviços.

A avaliação e classificação se baseiam em indicadores de desempenho, mantendo em seu cadastro somente aqueles que atendem os requisitos mínimos de qualidade determinados pelo Banco Mercantil A qualificação prévia dos fornecedores/empresas prestadoras de serviços a terceiros deve contemplar os aspectos legais, econômicos, patrimoniais, financeiros, fiscais e técnicos.

2.11. Gestão de vulnerabilidades

A gestão de vulnerabilidades tem como princípio a definição de uma ameaça tecnológica.

O objetivo desta atividade é determinar o impacto negativo resultante de um ataque bem-sucedido, isto é, o sucesso de uma ameaça explorando uma vulnerabilidade. Deve-se utilizar sistemas para realizar a gestão de vulnerabilidade de todos os ativos das empresas do grupo Mercantil.

Ameaça é a exploração de uma vulnerabilidade, de forma intencional ou não, cujo impacto poderá causar prejuízo financeiro ou influir na capacidade da empresa de alcançar seus objetivos ou ofertar seus serviços.

Os procedimentos e os controles adotados para reduzir a vulnerabilidade e a decorrência de incidentes e atender aos demais objetivos de segurança cibernética são aplicados também aos processos que envolvem o desenvolvimento de sistemas de informação seguros, bem como na adoção de novas tecnologias empregadas nas atividades da instituição.

São utilizadas no Banco Mercantil, ferramentas focadas em gestão de vulnerabilidades que monitoram em real time, além de conter regras e políticas de bloqueios em cada atividade suspeita, além de plataformas utilizadas como base de dados de ameaças e vulnerabilidades descobertas no ambiente interno e externo, visando bloquear os vetores de ataques já conhecidos.

Divulgação Externa

Com o objetivo de mitigar as ameaças de ataques cibernéticos é de responsabilidade da Gerência de Infraestrutura e Segurança de TI realizar periodicamente testes de intrusão, além de adotar controles na prevenção de vazamento de informação e contra softwares maliciosos.

2.12. Segurança Antimalware

Ferramentas antimalware (Antivírus, Antispyware, Antirootkit e Antitrojan) são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador.

Ainda que existam ferramentas específicas para os diferentes tipos de códigos maliciosos, muitas vezes é difícil delimitar a área de atuação de cada uma delas, pois a definição do tipo de código malicioso depende de cada fabricante e muitos códigos mesclam as características dos demais tipos.

Para delinear essas ameaças, todos os ativos das empresas do grupo Mercantil devem seguir o procedimento operacional de "Gestão da Solução Antimalware" disponível junto aos demais procedimentos de TI.

2.13. Classificação da Informação

A Classificação da informação é uma prática no ambiente nos serviços que requisitam de todo o conglomerado Mercantil, sendo regida por procedimentos específico que definem as ações próprias. Esse procedimento como título – "Classificação das Informações", pode ser consultada na Política de Segurança da Informação.

2.14. Gestão da Criptografia

Com o objetivo de manter a confidencialidade e a integridade de dados, o Banco Mercantil possui uma estratégia geral de criptografia que é ajustada para se adequar a diferentes aplicações e tipos de dados, de acordo com a criticidade e relevância avaliadas para cada cenário específico.

O processo de gestão é composto por uma combinação de procedimentos e controles tecnológicos, nos quais são considerados critérios que resultem em melhor desempenho e latência para os sistemas e ambientes do grupo, visando também a integração com outras ferramentas de segurança e a comunicação com sistemas legados e multiplataforma. Este processo contempla desde a definição de quais dados serão criptografados e a escolha das tecnologias mais eficazes, até o gerenciamento contínuo das chaves de criptografia. Serão protegidos os dados digitais que se encontram em repouso (que existem em mídia física) e em trânsito (transferidos entre componentes, locais ou sistemas).

A criação de chaves de criptografia e certificados digitais, após entendimento e avaliação pontual de cada necessidade, é de responsabilidade da Gerência de Infraestrutura e Segurança de TI. Cada chave ou certificado possui data de expiração definida, podendo ser renovado, revogado ou recuperado no decorrer do seu próprio ciclo de vida, de acordo com a determinação da área responsável por esta gestão. Ao final do ciclo de vida, todos os elementos são obrigatoriamente revogados, garantindo assim que os mesmos não poderão ser reutilizados em nenhuma outra circunstância.

Maiores informações podem ser encontradas na Política Institucional de Criptografia.

Divulgação Externa

2.15. Contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior

Os serviços relevantes que forem processados, armazenados ou utilizem de computação em nuvem em países do exterior, devem observar os seguintes requisitos.

- A existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;

- Que a prestação dos serviços não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;

- Informar os países e as regiões onde os serviços serão prestados bem como onde os dados são armazenados, processados e gerenciados;

- A obrigatoriedade, em caso de extinção do contrato, de realizar a transferência dos dados ao novo prestador de serviços ou à Instituição contratante, realizando posteriormente a exclusão definitiva dos dados em seu ambiente;

- Devem instituir mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade da Política de segurança cibernética, na qual devem abordar a definição de processos, testes e trilhas de auditoria, a definição de métricas e indicadores adequados.

A Gerência de Segurança Cibernética e da Informação terá a prerrogativa de vetar a contratação da empresa, caso a mesma não esteja em conformidade com os artigos 16 e 17

da Resolução CMN Nº 4.893/21.Vale ressaltar que, conforme estabelecido por esta Resolução, devem ficar à disposição do Banco Central do Brasil pelo prazo de 5 (cinco) anos:

- Os documentos para a contratação de serviços prestados no exterior.

- Os contratos e todas as informações, incluindo dados e registros, relativos aos mecanismos de acompanhamento e de controle instituídos com vistas a assegurar a implementação e a efetividade da política de segurança cibernética.

- Documento relativo ao plano de ação e de resposta a incidentes.

- Dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

- A documentação com os critérios que configurem a situação de crise, contendo os procedimentos adotados para gerenciamento de riscos, no tocante à continuidade dos serviços prestados.

Divulgação Externa

2.15.1. Serviços de Comunicação (RSFN)

Conforme determinado pela regulamentação vigente (Art. 22-B da Resolução CMN 4.893/21, introduzido pela Resolução CMN 5.274/25), todo serviço prestado para a comunicação eletrônica de dados na Rede do Sistema Financeiro Nacional (RSFN) é classificado mandatoriamente como Serviço Relevante. Esta classificação aplica-se independentemente da forma de conexão utilizada — seja por meio de links dedicados, redes virtuais privadas (VPN) ou internet — e estende-se inclusive aos prestadores que fornecem serviços de processamento de mensagens no âmbito do SFN e do Sistema de Pagamentos Brasileiro (SPB). Dessa forma, aplicam-se integralmente a estes contratos todos os requisitos de governança, contratação e segurança cibernética estabelecidos nesta política para serviços de processamento, armazenamento de dados e computação em nuvem.

2.16. Interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior

Na ocorrência de eventos que interrompam o serviço relevante de processamento, armazenamento de dados e de computação em nuvem, devem ser avaliadas as causas do ocorrido, se houve descumprimento por parte da contratada gerando o fato, se poderia ter sido evitado, assim como formas de mitigar uma recorrência daquela(s) atividade(s).

Conforme a Resolução nº 4.893/2021, o Banco Mercantil deve avaliar se a empresa contratada realizou os serviços de forma segura e aderente aos requisitos citados na

resolução. Caso seja detectado que houve descumprimento ou falha em um dos procedimentos que a resolução contempla, o contrato poderá ser interrompido respeitando:

- Um eventual pedido de prazo de trinta dias para a interrupção do serviço;
- A transferência dos dados ao novo prestador de serviço e/ou ao Banco Mercantil;
- A exclusão dos dados pela empresa contratada substituída, após a transferência e confirmação da integridade e disponibilidade dos dados.

Caso seja detectada inadimplência pelo Banco Mercantil, a empresa contratada também tem o direito de interrupção dos serviços, respeitando os prazos previstos na resolução.

2.17. Monitoramento de Conexões com Ambientes Externos e Eventos Atípicos

Em observância aos requisitos de segurança e controles de acesso, e em conformidade com as exigências da Resolução CMN 5.274/2026, a Instituição estabelece o monitoramento ativo e contínuo das conexões com ambientes externos.

Divulgação Externa

2.17.1. Critérios de Alerta

Devem ser definidos e mantidos critérios de alerta específicos para o estabelecimento e a manutenção de conexões externas, com especial vigilância para acessos realizados em:

I. Horário noturno: compreendido entre as 22h00 e as 06h00;

II. Dias não úteis: abrangendo finais de semana e feriados nacionais.

2.17.2. Caracterização de Eventos Atípicos

Toda conexão realizada fora dos padrões operacionais e perfis de acesso previamente autorizados será classificada como evento atípico.

2.17.3. Tratamento e Resposta

Os eventos identificados nos termos do item 2.8.1 devem ser encaminhados com prioridade alta para análise e tratamento imediato pelas equipes de Segurança Cibernética e Operações, observando-se o fluxo de escalonamento definido no MP-0529 Gestão de Registro de Logs e as diretrizes de acesso contidas no MP-0155 Acesso Remoto.

2.17.4. Registros e Evidências

Os logs e trilhas de auditoria referentes a estes acessos devem ser armazenados de forma a garantir sua integridade para fins de reporte e auditorias internas ou regulatórias. Grupo Mercantil estabelece as diretrizes fundamentais para a gestão de registros de logs, detalhando os procedimentos de coleta, armazenamento e análise de dados para garantir a segurança cibernética da instituição. O texto define responsabilidades claras entre as áreas de tecnologia e segurança, introduzindo conceitos técnicos essenciais como o uso de sistemas SIEM para o monitoramento proativo de ameaças em tempo real. Além de padronizar a infraestrutura técnica, a norma determina prazos de retenção específicos para diferentes tipos de registros, assegurando a conformidade com as exigências regulatórias do setor financeiro e a proteção de dados sensíveis. O propósito final é fortalecer a integridade e a auditabilidade das informações, permitindo investigações forenses eficazes e a detecção oportuna de comportamentos suspeitos ou incidentes de segurança, que por meio do manual de procedimentos MP-0529 - Gestão de registro de logs.

2.18. Disponibilidade e Retenção de Mecanismos de Controle (Compliance BACEN)

Em observância às obrigações de supervisão e transparência regulatória, as empresas do Grupo Mercantil asseguram a disponibilidade e a integridade das evidências de controle pelo período determinado pelo Banco Central do Brasil.

Divulgação Externa

2.18.1. Abrangência da Documentação

Devem ser mantidos à disposição do Banco Central do Brasil todos os dados, registros e informações que comprovem a efetividade dos mecanismos de acompanhamento e controle, incluindo, mas não se limitando a:

- **Trilhas de Auditoria e Testes:** Evidências de execução de processos e testes de segurança cibernética;
- **Métricas e Indicadores:** Relatórios de indicadores de desempenho (KPIs/KRIs) que demonstrem a saúde da política de segurança;
- **Gestão de Deficiências:** Registros que identifiquem falhas detectadas e as respectivas ações de correção implementadas;
- **Controle de Subcontratação:** Evidências de que as notificações de subcontratação de serviços relevantes (nuvem/processamento) foram consideradas na estrutura de controle;
- **Relatórios de Auditoria Interna:** Resultados dos testes periódicos realizados sobre os mecanismos de segurança cibernética.

2.18.2. Prazo de Guarda e Contagem:

- **Prazo Mínimo:** Todos os documentos e registros citados acima devem permanecer à disposição do regulador pelo prazo mínimo de 5 (cinco) anos.
- **Marco Inicial da Contagem:** Para os mecanismos de acompanhamento e controle, o prazo de cinco anos começa a ser contado a partir da data de implementação dos referidos mecanismos ou da geração do registro de controle. No caso de contratos de serviços de nuvem/processamento, o prazo de cinco anos conta-se a partir da extinção do contrato.

2.18.3. Condições de Armazenamento

As informações devem ser armazenadas de forma a garantir sua pronta exibição ao Banco Central do Brasil quando solicitadas, preservando o histórico evolutivo da política de segurança cibernética, do plano de ação e de resposta a incidentes.

2.19. Segurança nas Conexões com Sistemas do Mercado Financeiro

Em conformidade com os requisitos de segurança adicionais para participantes de Sistemas do Mercado Financeiro (SMF), a Instituição utiliza seus controles de criptografia (POL-0035 Política de Criptografia, monitoramento de logs (MP-529 Gestão de Registro de Logs) e gestão de incidentes (MP-0222 Plano e Ação de Resposta a Incidentes de Segurança) para prevenir, detectar e responder especificamente a tentativas de fraude nessas conexões. Este processo fundamenta-se na análise de comportamentos anômalos e na garantia da integridade das mensagens transacionadas, assegurando que as operações junto ao SMF ocorram em ambiente controlado e resiliente a fraudes.

Divulgação Externa

2.20. Uso de Correio Eletrônico e Dispositivos Móveis

O uso do sistema de correio eletrônico corporativo e seu respectivo acesso por meio de dispositivos móveis tem como objetivo viabilizar a comunicação e a troca de informações essenciais para as atividades profissionais do Grupo Mercantil. Este recurso é destinado exclusivamente para o desempenho das funções corporativas, sendo o colaborador o único responsável por todo o conteúdo enviado ou recebido através de sua conta.

Como diretrizes gerais de segurança, é terminantemente proibido o compartilhamento de credenciais de acesso, o tráfego de conteúdos inadequados, discriminatórios ou maliciosos, bem como o envio ou encaminhamento de informações corporativas para caixas postais externas e pessoais. O acesso às mensagens via dispositivos móveis deve ser realizado estritamente pelo aplicativo corporativo homologado pela instituição, respeitando o uso privado e confidencial da ferramenta. Adicionalmente, qualquer incidente que envolva a perda ou o furto de aparelhos móveis com o e-mail corporativo configurado deve ser notificado de forma imediata à área de segurança. As regras detalhadas de utilização, fluxos de aprovação e configurações técnicas complementares estão estabelecidas no normativo interno específico de Correio Eletrônico e Móvel, que atua de forma vinculada a esta Política por meio do manual de procedimento MP-0058 - Correio eletronico e móvel.

2.21. Descarte Seguro de Informações

O processo de descarte seguro de informações tem como objetivo principal garantir a destruição definitiva e irreversível dos dados produzidos e armazenados no ambiente corporativo, abrangendo tanto os formatos físicos quanto lógicos. Este procedimento é essencial para assegurar que informações críticas, dados pessoais, movimentações financeiras e documentos protegidos por sigilo bancário não sejam expostos, acessados ou recuperados por pessoas não autorizadas. O descarte seguro deve ser obrigatoriamente aplicado sempre que mídias digitais, equipamentos ou documentos impressos perderem sua utilidade, chegarem ao fim de sua vida útil, no término de contratos de aluguel de ativos ou quando houver a realocação de estações de trabalho.

Como diretriz geral, toda eliminação de informações confidenciais ou de uso restrito deve ser realizada por meio de métodos que impeçam totalmente a sua recuperação, seja pela exclusão lógica definitiva ou pela destruição física do material. A responsabilidade por esse processo é compartilhada: cabe a todos os colaboradores realizar o descarte seguro de documentos manuscritos ou impressos gerados em suas atividades, enquanto as áreas de tecnologia e de processamento ficam encarregadas de operacionalizar a exclusão estruturada em equipamentos, servidores e mídias removíveis, podendo, inclusive, contratar empresas especializadas para a destruição física quando necessário. As definições precisas de responsabilidades, os métodos de destruição aceitos e os critérios de avaliação estão detalhados no normativo interno específico de Descarte Seguro de Informações, que atua em conjunto com esta Política por meio do manual de procedimento MP-0155 - Acesso Remoto a Rede Corporativa do Grupo Mercantil.

Divulgação Externa

2.22. Acesso a Dados e Sistemas

O processo de gestão de acessos a dados e sistemas tem como objetivo principal proteger as informações corporativas, pessoais e sensíveis, garantindo que a entrada nos ativos tecnológicos do Grupo Mercantil seja concedida de forma estruturada, centralizada e estritamente baseada na função exercida por cada colaborador. Essa prática assegura que os usuários possuam apenas os privilégios mínimos necessários para o sucesso e a execução de suas atividades profissionais rotineiras. Como diretriz geral de segurança, as credenciais e senhas de acesso são de uso pessoal e intransferível, sendo terminantemente proibido o seu compartilhamento sob qualquer justificativa. Toda e qualquer concessão de acesso a bancos de dados, sistemas e aplicativos corporativos exige uma solicitação formal que deve passar, obrigatoriamente, por um fluxo de aprovação prévia dos gestores responsáveis pela área ou pela informação. Adicionalmente, todas as intervenções realizadas nas bases de dados são registradas em trilhas de auditoria (logs) para permitir o rastreamento integral das ações, identificar alterações e viabilizar o monitoramento contínuo de eventos suspeitos ou não autorizados. Para manter a integridade e a conformidade do ambiente, os acessos devem ser cancelados sempre que houver mudança de função e passam por revisões periódicas anuais. Nessas revisões, os gestores certificam formalmente a necessidade de manter ou revogar as permissões concedidas aos membros de suas equipes. Os fluxos detalhados de aprovação, ferramentas oficiais de requisição, prazos e tipos de perfis estão definidos no normativo interno de Acessos a Dados e Sistemas, que atua em conjunto com esta Política por meio do manual de procedimento MP-0165 - Acesso a Dados e Sistemas.

2.23. Acesso e Uso de Recursos da Internet

O processo de gestão de acesso aos recursos de internet tem como objetivo estabelecer as diretrizes e regras seguras para o fornecimento, utilização e controle da navegação web por todos os colaboradores, administradores e prestadores de serviços do Grupo Mercantil. Como diretriz geral, a concessão e a habilitação do acesso à internet são realizadas exclusivamente para a execução de atividades corporativas, sendo as credenciais de usuário e senha de uso estritamente pessoal e intransferível. A navegação e a troca de arquivos devem estar sempre alinhadas aos propósitos profissionais da instituição, sendo expressamente proibido o acesso a sites com conteúdos inadequados, ofensivos, ilícitos ou potencialmente maliciosos. Além disso, é vedada a utilização de hospedagens não autorizadas, compartilhadores de arquivos, bem como comunicadores instantâneos pessoais para fins de tráfego de dados corporativos ou confidenciais, a fim de mitigar riscos de infecção por códigos maliciosos e evitar o vazamento de dados.

Para assegurar a proteção do ambiente computacional e a produtividade, a instituição realiza o monitoramento automatizado e contínuo da utilização da rede. Este acompanhamento inclui a auditoria do tráfego, gestão do tempo de uso e o bloqueio proativo de páginas e arquivos considerados perigosos, indesejáveis ou que representem riscos à segurança. Qualquer necessidade de acesso a sites bloqueados ou liberação de ferramentas de comunicação em caráter de exceção dependerá de uma justificativa de negócio e deverá passar por um fluxo formal de aprovação pelas gerências responsáveis. As regras pormenorizadas sobre o uso consciente de mídia, limitações de transferência, navegadores homologados e o processo formal de requisição de acessos encontram-se estabelecidas no normativo interno específico de Recursos de Internet, que atua de forma complementar e vinculada a esta Política por meio do manual de procedimentos MP-0252 - Recursos de Internet.pdf.

Divulgação Externa

O Grupo Mercantil estabelece as diretrizes para a varredura de dados na internet, visando proteger informações corporativas e dados pessoais contra exposições indevidas. A instituição deve possuir uma estratégia de monitoramento contínuo que abrange desde redes sociais e fóruns até ferramentas de threat intelligence, buscando identificar proativamente possíveis vazamentos na web e na darkweb. Para garantir a segurança institucional, recomendasse que tenha um processo rigoroso de identificação e qualificação de dados, além de protocolar o tratamento e a comunicação de incidentes cibernéticos. Para a continuidade dos trabalhos deve-se ter uma governança para mitigar riscos digitais, assegurando que qualquer vulnerabilidade detectada seja prontamente analisada e contida pelas equipes de segurança, que atua de forma complementar e vinculada a esta Política por meio do manual de procedimentos MP-0351 - Varredura de dados na internet.

2.24. Credenciais Privilegiadas de Administrativas

O processo de gerenciamento de senhas de acesso tem como objetivo central estabelecer as regras e responsabilidades para a administração segura das credenciais dos usuários no ambiente de Tecnologia da Informação do Grupo Mercantil. Como diretriz geral e inegociável de segurança, a senha de acesso a qualquer ambiente da rede corporativa é de uso estritamente pessoal e intransferível. Cada usuário assume total e direta responsabilidade por todas as atividades, registros e operações realizadas sob a sua conta. Para preservar a integridade do ambiente, é terminantemente proibido o compartilhamento de senhas ou credenciais entre funcionários e prestadores de serviços, sendo igualmente vedado solicitar, divulgar ou fornecer a senha a terceiros sob qualquer pretexto ou justificativa.

Visando manter um ambiente protegido contra acessos não autorizados, as credenciais devem obedecer a critérios específicos de formação estrutural e necessitam ser alteradas obrigatoriamente em períodos pré-estabelecidos. Como medida preventiva adicional, contas que não forem utilizadas por um longo período ou que apresentarem falhas consecutivas e suspeitas de digitação serão automaticamente bloqueadas pelo sistema. As regras técnicas de complexidade, bem como os procedimentos sistêmicos e centralizados para o primeiro acesso, troca e desbloqueio seguro de usuários, encontram-se detalhados no normativo interno específico de Senhas de Acesso à Rede Corporativa, que atua em estrita conformidade e de forma vinculada a esta Política, que atua de forma complementar e vinculada a esta Política por meio do manual de procedimentos MP-0506 Senhas de acesso a rede corporativa.

2.25. Senhas de Acesso à Rede Corporativa

Em conformidade com os requisitos de segurança adicionais para participantes de Sistemas do Mercado Financeiro (SMF), a Instituição utiliza seus controles de criptografia (POL-0035 Política de Criptografia, monitoramento de logs (MP-529 Gestão de Registro de Logs) e gestão de incidentes (MP-0222 Plano e Ação de Resposta a Incidentes de Segurança) para prevenir, detectar e responder especificamente a tentativas de fraude nessas conexões. Este processo fundamenta-se na análise de comportamentos anômalos e na garantia da integridade das mensagens transacionadas, assegurando que as operações junto ao SMF ocorram em ambiente controlado e resiliente a fraudes.

Divulgação Externa

2.26. Pentest e Teste de Vulnerabilidade

O processo de realização de testes de penetração (pentest) e avaliações de vulnerabilidade tem como objetivo principal garantir a segurança, a estabilidade e a resiliência dos aplicativos, sistemas e infraestrutura do Grupo Mercantil. Essa prática busca identificar, avaliar e corrigir preventivamente eventuais fragilidades antes que possam ser exploradas por agentes maliciosos, minimizando o risco de indisponibilidade ou comprometimento dos serviços. Em estrita conformidade com as exigências regulatórias do Banco Central do Brasil, a execução periódica de testes de intrusão é obrigatória e deve ser conduzida de forma a garantir a total independência e imparcialidade dos resultados, exigência que pode ser cumprida por meio da contratação de empresas externas especializadas.

Como diretriz geral de segurança, as avaliações devem contemplar os componentes internos e externos do ambiente computacional e ocorrer não apenas de maneira programada, mas também de forma proativa sempre que houver mudanças significativas, como o lançamento de novas funcionalidades, refatoração de códigos ou alterações na infraestrutura exposta à internet. Todas as vulnerabilidades descobertas durante os testes são tratadas com o mais alto grau de confidencialidade e submetidas a uma rigorosa classificação de risco. Essa classificação orienta a prioridade das medidas de correção e remediação por parte das equipes responsáveis. As regras pormenorizadas sobre o escopo das avaliações, prazos para correção de falhas e as modalidades de testes aplicáveis encontram-se estabelecidas no normativo interno específico de Pentest e Teste de Vulnerabilidade, que atua de forma complementar e vinculada a esta Política, que por meio do manual de procedimentos MP-0521 - Pentest e Teste de Vulnerabilidade.

2.26.1. Plano Simulado de Ataques Ciberneticos

O Grupo Mercantil, detalhando as estratégias e procedimentos para testar a resiliência tecnológica de suas empresas. O documento organiza um cronograma de testes de invasão, simulações de phishing e exercícios de crise, conhecidos como "War Games", visando identificar vulnerabilidades e aprimorar a capacidade de resposta da equipe. A estrutura define responsabilidades específicas para as áreas de infraestrutura e segurança, além de estipular prazos rigorosos para a correção de falhas baseados em sua criticidade. O propósito central é fortalecer a cultura de segurança digital e garantir a proteção dos dados institucionais por meio de uma avaliação contínua e técnica de possíveis ameaças, que está vinculado a essa política por meio da MP-0602 Plano Simulado de Ataques Ciberneticos.

2.27. Gestão de Vulnerabilidades e Patch Management

Em conformidade com os requisitos de segurança de um ambiente tecnológico, o processo de Gestão de Vulnerabilidades e Patch Management tem como objetivo principal garantir a segurança, a proteção de dados e a integridade de todos os sistemas de informação e ativos tecnológicos do Grupo Mercantil contra ameaças e ataques cibernéticos crescentes. A adoção contínua desta prática visa identificar, classificar e corrigir proativamente eventuais falhas sistêmicas presentes em sistemas operacionais, aplicativos, bancos de dados e equipamentos de rede, independentemente de estarem localizados fisicamente na instituição, na nuvem ou em dispositivos móveis.

Divulgação Externa

Como diretriz geral de segurança, todas as vulnerabilidades identificadas no ambiente corporativo por meio de varreduras devem ser rigorosamente avaliadas e priorizadas com base em padrões de mercado que mensuram a severidade, a facilidade de exploração e o impacto potencial para a confidencialidade e disponibilidade do negócio. Essa classificação de criticidade dita a urgência e os prazos exigidos para a aplicação das correções (patches) aplicáveis.

A condução desse processo é colaborativa e contínua: cabe à área de Segurança Cibernética o monitoramento, a identificação e a priorização dos riscos, enquanto as equipes de Infraestrutura e Processamento são responsáveis por garantir o funcionamento das ferramentas de distribuição, realizar testes prévios de compatibilidade e operacionalizar a aplicação segura das atualizações nos ambientes de produção. Adicionalmente, todo o ciclo deve prever planos de reversão em caso de falhas (rollback) e ser documentado por meio de relatórios periódicos, garantindo a rápida mitigação e a minimização do tempo em que os sistemas ficam expostos. As matrizes detalhadas de níveis de risco, prazos de atendimento (SLA) esperados e métricas de avaliação encontram-se estabelecidas no normativo interno específico de Gestão de Vulnerabilidades e Patch Management, que atua de forma complementar e vinculada a esta Política por meio do manual de procedimentos MP-0523 - Gestão de Vulnerabilidades e Patch Management

2.28. Acesso Remoto a Rede Corporativa do Grupo Mercantil

O processo de gerenciamento de acesso remoto tem como objetivo principal estabelecer as diretrizes e os controles para a conexão segura aos recursos tecnológicos e infraestrutura interna do Grupo Mercantil a partir de ambientes externos. Esta modalidade de conexão é disponibilizada exclusivamente para fins profissionais, sendo permitida apenas quando a natureza das atividades do colaborador, terceiro ou parceiro de negócio de fato exigir esse recurso. Como regra geral de segurança, a habilitação de qualquer acesso remoto não é automática; ela requer uma solicitação formal, aprovação prévia conjunta das áreas gestoras e de segurança, e a concordância formal por meio da assinatura de um termo de responsabilidade.

Para garantir a proteção contínua do ambiente cibernético da instituição, os acessos concedidos são submetidos a um monitoramento ativo e contínuo. Conexões realizadas em horários noturnos, finais de semana ou feriados são automaticamente classificadas como eventos atípicos e tratadas com prioridade alta pelas equipes de segurança. Além disso, como mecanismo de controle de privilégios, todos os acessos remotos devem ser recertificados anualmente pelos gestores solicitantes, que atestam a real necessidade de manutenção do recurso. O acesso deve ser bloqueado ou imediatamente revogado em casos de desligamento, mudança funcional, afastamento ou quando a justificativa inicial do uso deixar de existir. Para fins de rastreabilidade e auditoria, todos os registros e trilhas das conexões são armazenados de forma segura pelo período mínimo de cinco anos. Os critérios pormenorizados de aprovação, modalidades de conexão aceitas e as ferramentas homologadas encontram-se estabelecidos no normativo interno específico de Acesso Remoto à Rede Corporativa, que atua de forma inseparável e estritamente vinculada a esta Política por meio do manual de procedimentos MP-0155 - Acesso Remoto a Rede Corporativa do Grupo Mercantil

Divulgação Externa

2.29. Plano de Ações de Respostas a Incidentes

O processo de Plano de Ações de Respostas a Incidentes tem como objetivo central formalizar e detalhar as diretrizes para a gestão, mitigação e recuperação diante de crises ou ameaças envolvendo a segurança cibernética, a segurança da informação e possíveis vazamentos de dados pessoais no âmbito do Grupo Mercantil. A adoção rigorosa destas diretrizes visa interferir o mínimo possível nas operações do negócio, minimizar potenciais consequências aos titulares de dados, proteger as operações financeiras e reduzir os custos diretos e indiretos atrelados a violações. Este planejamento preventivo e reativo estabelece um fluxo corporativo padronizado que orienta de ponta a ponta as equipes responsáveis, cobrindo desde a identificação e notificação inicial de um evento anômalo até a fase final de contenção, recuperação e aprendizado.

Como diretriz geral de execução, o tratamento de incidentes deve ocorrer mediante uma investigação imparcial e independente, baseada em evidências sólidas e com garantia da preservação de provas digitais por meio de perícia forense. Havendo a confirmação de um incidente, um Comitê de Crise é estruturado e acionado para assumir a coordenação centralizada da resposta, sendo o responsável por tomar as decisões estratégicas de alto nível para proteger a instituição e seus clientes. É importante ressaltar que a política institucional recomenda expressamente a não negociação ou pagamento a criminosos em casos de pedidos de resgate de dados (como em ataques de sequestro digital), salvo em situações extremamente atípicas de impacto operacional crítico que demandem essa reavaliação pela alta gestão.

Para que a resposta seja proporcional à ameaça, todo incidente de segurança é obrigatoriamente categorizado e priorizado com base em seu impacto. A classificação leva em consideração a natureza e a sensibilidade das informações comprometidas, a existência de dados pessoais e a interrupção gerada nas funções críticas do negócio. Um dos pilares mais essenciais neste processo é a comunicação corporativa: o Grupo Mercantil zela pela transparência e rapidez, possuindo fluxos definidos para notificar tempestivamente todos os atores necessários de acordo com a gravidade do cenário. Isso engloba comunicações obrigatórias para os órgãos reguladores — como o Banco Central do Brasil, a Autoridade Nacional de Proteção de Dados (ANPD) e a Comissão de Valores Mobiliários (CVM) —, além de reportes claros aos titulares afetados, investidores, comunidade externa e imprensa.

Finalizadas as etapas críticas de erradicação da ameaça e restauração validada dos sistemas afetados, o ciclo de gestão foca no fortalecimento das defesas e na melhoria contínua. A fase de pós-incidente exige a formulação de relatórios consolidados abordando a causa raiz, os sistemas impactados e o comportamento das defesas. As lições aprendidas derivam ações de melhoria sistêmica, como o ajuste de controles em firewalls, a aplicação de correções definitivas e a atualização dos programas de treinamento de conscientização em segurança para os colaboradores. Visando manter o estado de alerta e a fluidez desse processo, a organização também exige a realização periódica de simulações e exercícios práticos de crise, garantindo a prontidão das equipes para o mundo real. As definições exatas sobre as matrizes de responsabilidade de cada área, os limites de tempo aceitáveis e os formulários oficiais de notificação regulatória estão documentados no normativo interno específico do Plano de Ações de Respostas a Incidentes, que atua de forma inseparável a esta Política por meio do manual de procedimentos MP-0222 Plano de Ações de Respostas a Incidentes.

Divulgação Externa

2.29.1. Checklist de Acoes de Seguranca Cibernetica

O Grupo Mercantil deve padronizar a resposta a incidentes cibernéticos, visando reduzir erros humanos e garantir a continuidade do negócio. A estrutura organiza-se cronologicamente em um checklist de ações que abrangem os períodos anterior, simultâneo e posterior a um ataque, detalhando procedimentos de erradicação de ameaças e restauração de sistemas. O item deve ser multidisciplinar, integrando respostas técnicas, gerenciais, jurídicas e de comunicação para mitigar danos de forma holística. Por fim, deve-se priorizar o aprendizado organizacional, exigindo a análise de lições aprendidas e a revisão de controles para fortalecer a resiliência digital contra futuras vulnerabilidades, que está vinculado a essa política por meio da MP-0558 Checklist de Acoes de Seguranca Cibernetica.

3. PAPÉIS E RESPONSABILIDADES

Os papéis e responsabilidades atinentes a esta Política estão distribuídos entre as alçadas abaixo indicadas:

- Conselho de Administração ou Diretoria
- Comitê de Riscos
- Comitê Executivo
- Superintendência de Tecnologia
- Gerência de Segurança Cibernética e da Informação
- Gerência de Processamento
- Gerência de Marketing
- Gerência de Risco Operacional e Controles Internos
- Gestores e proprietários de informações
- Todos os colaboradores
- Fornecedores e Prestadores de Serviços
    - Garantir o acesso aos dados e às informações a serem processados ou armazenados pela empresa em data center próprio ou na modalidade de nuvem;
    - Garantir a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processadas ou armazenadas pela empresa;
    - Manter-se aderente às certificações exigidas para a prestação do serviço a ser contratado;

Divulgação Externa

- Disponibilizar ao Banco Mercantil e ao Banco Central do Brasil, quando solicitados, os relatórios elaborados por empresa de auditoria especializada independente, relativos aos procedimentos e aos controles utilizados na prestação dos serviços;

- Assegurar o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

- Identificar e segregar os dados das empresas do Grupo Mercantil por meio de controles físicos ou lógicos e estabelecer processo periódico de auditoria e monitoramento que garantam esta segregação de dados;

- Garantir a qualidade dos controles de acesso voltados à proteção dos dados e das informações;

- Adotar controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo, no caso de aplicativos implantados ou desenvolvidos pela empresa com a utilização de recursos computacionais da própria empresa;

- Indicar os países e as regiões em cada país onde os serviços serão prestados e onde os dados serão armazenados, processados e gerenciados;

- Adotar medidas de segurança para a transmissão e armazenamento dos dados;

- Garantir, no caso de extinção deste contrato, a transferência dos dados ao novo prestador de serviços ou ao Banco Mercantil;

- Informar ao Banco Mercantil sobre a subcontratação de serviços a serem fornecidos pela empresa;

- Permitir o acesso ao Banco Central do Brasil aos contratos e aos acordos firmados para prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações pelo período de 5 anos;

- Ajustar os processos da empresa caso haja determinação do Banco Central do Brasil;

- Manter o Banco Mercantil permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

- Auditoria Interna

Divulgação Externa

4. CONSIDERAÇÕES FINAIS

Esta Política deve ser objeto de avaliação periódica, com o intuito de que seja continuamente aprimorada e de esteja sempre atualizada.

Este documento entra em vigor a partir de sua publicação, ficando à disposição dos órgãos de fiscalização e supervisão.

5. REFERÊNCIAS NORMATIVAS

Tipo	Número/Ano	Objetivo
Resolução CMN	5.274/25	Atualiza o marco de segurança cibernética para instituições autorizadas pelo Banco Central, fortalecendo controles, rastreabilidade e gestão de riscos em nuvem e TI.
Resolução CMN	4.893/21	Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.
Resolução BCB	85/21	Trata-se dos requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.
Resolução CVM	35/21, 134/22, 179/23 e 196/23	Dispõe sobre incidente relevante de segurança que afete processos críticos de negócios, ou dados ou informações sensíveis, e tenha impacto significativo sobre os clientes

6. GLOSSÁRIO

- Phishing: Forma de fraude online na qual indivíduos mal-intencionados tentam enganar pessoas para obter informações confidenciais, como senhas, números de cartão de crédito ou detalhes de conta.Isso geralmente é feito por meio de mensagens eletrônicas, sites falsos ou outras técnicas enganosas que se fazem passar por entidades confiáveis, induzindo as vítimas a revelarem dados pessoais.

- Smishing: Forma de ataque de phishing que ocorre por meio de mensagens de texto (SMS). Os cibercriminosos enviam mensagens fraudulentas, geralmente se passando por instituições legítimas, na tentativa de enganar as vítimas e induzi-las a fornecer informações confidenciais, clicar em links maliciosos ou realizar ações prejudiciais através de seus dispositivos móveis. O termo "smishing" deriva da combinação de "SMS" (Short Message Service) e "phishing".

- Vishing: Uma combinação das palavras "voice" (voz) e "phishing" (pesca), refere-se a uma prática de engenharia social em que os criminosos usam técnicas de manipulação por telefone para obter informações confidenciais das vítimas.

Divulgação Externa

–ABRANGÊNCIA–

Esta Política abrange a(s) seguinte(s) empresa(s) do Grupo Mercantil[1]:

Banco Mercantil de Investimentos S.A.; Banco Mercantil do Brasil S.A.; Bem Aqui - Administradora e Correta de Seguros, Previdência Privada e Correspondente Bancário S.A.; Domo - Digital Tecnologia S.A.; MBMKTP - Mercantil do Brasil Marketplace e Empreendimentos Imobiliários S.A.; Mercantil do Brasil Distribuidora S.A. - Títulos e Valores Mobiliários; Mercantil Financeira S.A. - Sociedade de Crédito, Financiamento e Investimento

A ciência e o cumprimento das diretrizes e regras deste normativo são obrigatórios a:

Terceiros (fornecedores, prestadores de serviços, parceiros de negócio, agentes intermediários e associados, donatários, patrocinados, acionistas e demais terceiros) das empresas do Mercantil acima citadas; Todos os colaboradores das empresas do Mercantil acima citadas (administradores, empregados e estagiários, independentemente de cargo ou função exercidos)

-

[1] Empresas que compõem o Grupo Mercantil:
Empresas operacionais: MB+, BMI, MC, MD, MF, Domo, Bem Aqui, MBMKTP
Empresas não operacionais: Sansa, Macs, Cosefi, e Fundos MB BI e MB FII.